ABSTRACT

Embodiments of the invention may be used to provide an authentication and key agreement protocol that is more robust against base station, replay and other attacks compared to previously known systems. The nonce-based authentication and key agreement protocol provides security against such attacks while avoiding the problems that arise in systems that use sequence number counters on the home environment and mobile station-sides. In an embodiment, a nonce that is transmitted from the user to the home environment through the serving network, as well as subsequent values for the nonce that are derived from the initial nonce, are used as indices for authentication vectors.